APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
08/999,766	07/23/97	MOSKOWITZ	S	2377/23

```
┌ KENYON & KENYON                LM71/0907        ┐
  1025 CONNECTICUT AVENUE NW
  WASHINGTON DC 20036
└                                                 ┘
```

EXAMINER
MEISLAHN, D

ART UNIT	PAPER NUMBER
2767	

DATE MAILED: 09/07/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

☒ Responsive to communication(s) filed on *Jul 23, 1998* .

☐ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire ___3___ month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *25-61* is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *25-61* is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐approved ☐disapproved.

☒ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____ .

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____ .

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). ___2___

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

Specification

1.   A substitute specification excluding claims is required pursuant to 37 CFR 1.125(a)

because the quality of the specification's print is poor.

A substitute specification filed under 37 CFR 1.125(a) must only contain subject matter

from the original specification and any previously entered amendment under 37 CFR 1.121. If the

substitute specification contains additional subject matter not of record, the substitute

specification must be filed under 37 CFR 1.125(b) and must be accompanied by: 1) a statement

that the substitute specification contains no new matter; and 2) a marked-up copy showing the

amendments to be made via the substitute specification relative to the specification at the time the

substitute specification is filed.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and
> distinctly claiming the subject matter which the applicant regards as his invention.

3.   Claims 46-49 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention. Claim 29, from which 46 depends, talks about decoding data, while 46 says that data is to be encoded. This seems contradictory. The examiner has treated the data as though claim 46 states that data is to be decoded.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371© of this title before the invention thereof by the applicant for patent.

5.   Claims 25, 28, 29, 32, 33, 35, 38, and 39 are rejected under 35 U.S.C. 102(e) as being anticipated by Braudaway et al. (5530759).

Braudaway et al. talk about using a random or pseudo-random key in the process of putting a watermark into data in lines 21-26 of the seventh column.

Lines 56-57 of column one say that there are watermarks that identify copyright owners.

By watermarking the data, Braudaway et al.'s method creates a first derivative encoded signal. It is inherent that attempts to decode the watermark without the proper key would further obfuscate the information. It was once theorized that encrypting information with two keys in order to strengthen security could in fact be mimicked by using one key which would possibly be easier to break. Although this theory has since been proven incorrect, the immediate solution was

to strengthen security by encrypting with a first key and then decrypting with a non-corresponding

second key.

In the abstract, Braudaway et al. say that certain pixels brightness are altered as a result of

the watermark. This change in brightness anticipates claim 38's spectral values. Also in the

abstract, Braudaway et al. talk about using only certain non-transparent values of the watermark.

These non-transparent values form a map to meet claim 39.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

7.   Claims 25, 29, 33, 35, 40-43, and 46-48 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Schneier (*Applied Cryptography*, 1994).

On page 67, Schneier talks about encrypting subliminal data into a message using a

symmetric key. This is equivalent to encoding independent information into a signal. Official

notice is taken that digital watermarks, which imperceptibly incorporate data about information

into that information, are old and well-known as subliminal data used to authenticate documents.

Therefore it would have been obvious to a person of ordinary skill in the art at the time the

invention was made to make the subliminal data of Schneier a digital watermark capable of authenticating information.

Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

8.   Claims 26 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier or Braudaway et al. as applied to claims 25 and 29 above and further in view of Barton (5912972).

Schneier and Braudaway et al. teach encrypting digital watermarks into information with a key. They do not say that the information includes a stream of digital samples. Barton's teaches embedding authentication information within a stream of digital data. Therefore it would have

been obvious to a person of ordinary skill in the art at the time the invention was made to

authenticate digital sample streams as in Barton with the key-encrypted watermarks of Schneier.

9.   Claims 27 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier

or Braudaway et al. as applied to claims 25 and 29 above.

Schneier and Braudaway et al. teach encrypting digital watermarks into information with a

key. They do not say that the information includes a continuous analog waveform. Official notice

is taken that continuous analog waveforms are old and well-known. Since they can carry

information, continuous analog waveforms sometimes need to be authenticated. Therefore it

would have been obvious to a person of ordinary skill in the art at the time the invention was

made to authenticate continuous analog waveforms with the key-encrypted watermarks of

Schneier.

10.   Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier or

Braudaway et al. as applied to claim 33 above.

Schneier and Braudaway et al. teach encrypting digital watermarks into information with a

key. They do not say that the information is then modified. Encryption modifies data. Official

notice is taken that encrypting information in order to protect the data from unauthorized viewing

is old and well-known. Therefore it would have been obvious to a person of ordinary skill in the

art at the time the invention was made to protect the watermarked data of Schneier by encrypting

it.

11.   Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Braudaway et al.

or Schneier as applied to claim 29 above and further in view of Morris (5530751).

Schneier and Braudaway et al. teach encrypting digital watermarks into information with a

key. They do not say that one bit is read out of every sample for the watermark. In lines 50-52 of

the third column, Morris says that the human ear cannot detect the difference between a sound

value of 64000 and 64001. This would be a one-bit change of the least significant bit. As taught

by Morris, these small changes can be used to carry identification codes. Therefore it would have

been obvious to a person of ordinary skill in the art at the time the invention was made to

discretely carry the watermark information or Braudaway et al. or Schneier in the least significant

bits as taught by Morris.

12.   Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier or

Braudaway et al. as applied to claim 29 above, and further in view of Powell et al. (5930377).

Schneier and Braudaway et al. teach encrypting digital watermarks into information with a

key. They do not say that samples are mapped to extract bits of information. As is explained in

their abstract and diagrams, Powell et al. teach a method of embedding a digital watermark which

requires use of a map of an image to determine the places to embed the watermark. This method

is advantageous because, as explained in lines 42-43 of column 1, it is resistant to image

modification. Therefore it would have been obvious to a person of ordinary skill in the art at the

time the invention was made to employ the mapping techniques of Powell to the encryption

system of Schneier or Braudaway et al. so as to make the data's watermark resistant to data
modification.

13.   Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over
Schneier or Braudaway et al. as applied to claims 43, 44, and 48 respectively above, and further in
view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

        Schneier and Braudaway et al. teach encrypting digital watermarks into information with a
key. They do not say that the data is spectrally spread before insertion of the digital watermarked.
In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of
watermark removal, and robustness, of their system of spectrally spreading data, inserting the
watermark, and then putting the watermarked data through an inverse spectral spread. Therefore
it would have been obvious to a person of ordinary skill in the art at the time the invention was
made to reap the benefits of Cox et al.'s method in Schneier or Braudaway et al.'s system.

14.   Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over
Schneier or Braudaway et al. as applied respectively to claims 41 and 48 above, and further in
view of Barton (5912972).

        Schneier and Braudaway et al. teach encrypting digital watermarks into information with a
key. They do not say that a digital signature or hash of the start of message delimiter is validated.
In his second figure, Barton shows a digital signature being used as an authentication tool. Digital
signatures are made so that they are unique to the article which they authenticate. Therefore it
would have been obvious to a person of ordinary skill in the art at the time the invention was

made to use a digital signature, as taught by Barton, to verify the message sent by Schneier or

Braudaway et al.

15.   Claims 52-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier or

Braudaway et al. as applied to claim 25 above and further in view of Barton (5912972).

        Schneier and Braudaway et al. teach encrypting digital watermarks into information with a

key. They do not say that each sample has unique watermark information. In lines 20-33 of

column 4, Barton teaches including sequence data with the authentication data. The

authentication data is a reduced representation of digital data. Therefore it would have been

obvious to a person of ordinary skill in the art at the time the invention was made to uniquely

identify different samples so that the samples can be placed in the correct order. Unique

watermarks could also deter cryptanalysis attacks.

        Pre-processing sample windows is inherent, as is determining which and how many

windows will contain watermark information.

16.   Claims 56-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier or

Braudaway et al. as applied to claim 55 above.

        Schneier and Braudaway et al. teach encrypting digital watermarks into information with a

key. They do not say that the data that is watermarked is hashed and attached to itself. Official

notice is taken that hashing data and then attaching the hash to the data is old and well-known.

The hash acts as a verification. Digital signatures with message appendix are a common term

implementation of this. Therefore it would have been obvious to a person of ordinary skill in the

Application/Control Number: 08999766

Page 10

Art Unit: 2767

art at the time the invention was made to attach a hash of the information to the information. This

hash would be used to verify the integrity of the information.

Conclusion

17.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure. Conley (5894521) talks about hiding encryption data as a digital image.

Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Douglas Meislahn whose telephone number is (703) 305-1338. The

examiner can normally be reached Monday-Thursday and every other Friday from 8:30 AM to

6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,
Tod Swann, can be reached at (703) 308-7791.

The fax number for Formal or Official faxes to Technology Center 2700 is (703) 308-9051
or 9052. Draft or Informal faxes for this Art Unit can be submitted to (703) 305-0040.

Any inquiry of a general nature or relating to the status of this application should be
directed to the Group receptionist whose telephone number is (703) 305-3900.

DJM
August 30, 1999

GILBERTO BARRON, JR.
PRIMARY EXAMINER
ART UNIT 222 2767